

Effective model-completeness for p -adic analytic structures

Nathanaël Mariaule

Abstract

In this paper, we combine classical techniques of model theory of p -adic subanalytic sets with results of tropical analytic geometry to obtain a result of effective model-completeness. We consider languages $\mathcal{L}_F = (+, \cdot, 0, 1, P_n, f; n \in \mathbb{N}, f \in F)$ where F is a family of restricted analytic functions. Definable sets in this language are a collection of p -adic subanalytic sets. The main result of the paper gives conditions on F so that the structure with underlying set \mathbb{Z}_p in this language is effectively model-complete. An interesting example of language satisfying our hypotheses is the case where $F = \{\exp(px)\}$. This example gives a structure of exponential ring to \mathbb{Z}_p which is a natural p -adic equivalent to the (restricted) real exponential field.

1 Introduction

Let \mathcal{L}_{an} be the expansion of the language of rings by unary predicates for the set of n th powers and function symbols for all restricted p -adic analytic function (i.e. functions defined by power series convergent on \mathbb{Z}_p). The model theory of \mathbb{Z}_p in this language was first considered in J. Denef and L. van den Dries [2]. In particular, they proved that this theory admits the elimination of quantifiers if we expand \mathcal{L}_{an} by a symbol of division D . Definable sets in their language are the p -adic subanalytic sets. In this paper, we consider reduct of this language i.e. let F be any family of restricted analytic functions, we consider \mathcal{L}_F the expansion of the language of rings by predicates for the set of n th powers and function symbols for each $f \in F$. For instance, if $F = \{\exp(px)\}$, then \mathcal{L}_F induces a structure of exponential ring on \mathbb{Z}_p (which can be thought as the p -adic equivalent of the structure $(\mathbb{R}, +, \cdot, 0, 1, <, \exp|_{[-1,1]})$).

It follows from [2] that if F is a Weierstrass system (meaning roughly that it is closed under Weierstrass division, see section 2), then the theory of \mathbb{Z}_p admits quantifier elimination in the language \mathcal{L}_F expanded by the symbol of division. For general F , it seems very unlikely that the theory of \mathbb{Z}_p in this language also admits quantifier elimination. In this paper, we give conditions so that this theory admits the next best thing after quantifier elimination: strong model-completeness.

Definition 1.1. Let \mathcal{M} be a \mathcal{L} -structure with underlying set M . We say that \mathcal{M} is strongly model-complete if for any \mathcal{L} -formula $\Psi(\bar{y})$, there is an existential \mathcal{L} -formula $\exists \bar{x}\Phi(\bar{x}, \bar{y})$, where Φ is quantifier-free, such that for all $\bar{a} \in M^n$,

$$\mathcal{M} \models \Psi(\bar{a}) \leftrightarrow \exists \bar{x}\Phi(\bar{x}, \bar{a}),$$

and furthermore, for each \bar{a} such that $M \models \Psi(\bar{a})$, there is a unique tuple \bar{b} in M^m such that $M \models \Phi(\bar{b}, \bar{a})$.

A set X is strongly definable if

$$X = \{\bar{a} \in M^n \mid \mathcal{M} \models \exists \bar{y}\Phi(\bar{a}, \bar{b}, \bar{y})\},$$

and, for each $\bar{a} \in X$, there is a unique tuple \bar{c} in M^m such that $M \models \Phi(\bar{a}, \bar{b}, \bar{c})$. A function is strongly definable if its graph and the complement of its domain are strongly definable.

Note that in particular, any theory which eliminates the quantifiers is strongly model-complete. Our first main theorem is:

Theorem 5.2. Let F be a family of restricted analytic functions. Assume that the set of \mathcal{L}_F -terms is closed under derivation. Let \tilde{F} be the extension of F by the decomposition functions of each $f \in F$. Then, $\mathbb{Z}_{p, \tilde{F}}$ is strongly model-complete in $\mathcal{L}_{\tilde{F}}$.

This theorem was first proved by A. Macintyre [4] in the special case $F = \{(1+p)^x\}$ and the ideas of the proof goes back to L. van den Dries [7].

The main idea is to construct a Weierstrass system W_F which contains F and such that any element $f \in W_F$ is strongly definable in \mathcal{L}_F . We give the definition of this Weierstrass system in section 3 and prove the strong definability of its elements in section 5.

In the real case [7], the key property is that the structure $(\mathbb{C}, +, \cdot, \exp, \sin, \cos)$ is definable in $(\mathbb{R}, +, \cdot, \exp, \sin, \cos)$. In the p -adic case, the algebraic closure is an extension of infinite degree and therefore is not definable. But it is sufficient to interpret the natural structure attached to the valuation ring of any finite algebraic extension i.e. we want that the structure $(V, +, \cdot, 0, 1, f; f \in F)$ is \mathcal{L}_F -definable in \mathbb{Z}_p for any V valuation ring of a finite algebraic extension K . In general it may not be the case and so we expand F by a family of function called the *decomposition functions* so that $(V, +, \cdot, 0, 1, f; f \in \tilde{F})$ becomes definable (see section 4). Once we consider this expansion of the language, finite algebraic extensions are definable and the proof of the first theorem follows roughly by mimicking the proof in the real case.

The second main theorem concern the effectiveness of the first theorem i.e. it gives conditions so that we can compute explicitly an existential formula equivalent to a given \mathcal{L}_F -formula. The main issue comes from the proof of the quantifier elimination in [2]: a key lemma of this proof relies

on the Noetherian property of $\mathbb{Z}_p\{\overline{Y}\}$ and therefore is not effective. We give conditions on F so that we can overcome this Noetherian property. Basically, we show that if we don't need to use the Noetherian property at the level of \mathcal{L}_F -terms then we don't need it for the whole Weierstrass system W_F . And therefore,

Theorem 8.1. *Let F be an effective family of restricted analytic functions such that the set of \mathcal{L}_F -terms is closed under derivation. Let \tilde{F} be the extension of F by all decomposition functions of elements in F . Assume that each $\mathcal{L}_{\tilde{F}}$ -term is convergent on a open ball $B(f)$ containing \mathcal{O}_p and has an effective $B(f)$ -Weierstrass bound.*

Then, the theory of $\mathbb{Z}_{p,\tilde{F}}$ is effectively strongly model-complete in the language $\mathcal{L}_{\tilde{F}}$.

We discuss with more details this issue in section 6 and prove the theorem in section 8. In particular, we will relate the existence of this so-called effective Weierstrass bound to an (effective) counting point theorem in \mathbb{C}_p . We prove this counting point theorem in section 7 using results of tropical analytic geometry due to J. Rabinoff [6].

Remark. All the results of this paper remains valid if we replace \mathbb{Z}_p by the valuation ring of a finite algebraic extensions of \mathbb{Q}_p . As the proofs of this case are straightforward from our case, we will do our proof in the case \mathbb{Z}_p to keep the notations simpler.

Note that there are also versions of our results in the rigid case (i.e. for \mathbb{C}_p). In that case, we need to work with the ring of separated power series instead of $\mathbb{Z}_p\{\overline{X}\}$ and use the quantifier elimination due to L. Lipshitz [3]. Using our method and Lipshitz's quantifier elimination, one can prove a result of effective model-completeness.

Notations. Within this text, \mathbb{Q}_p will denote the field of p -adic numbers. We will denote the p -adic valuation by v . \mathbb{C}_p will denote the p -adic completion of the algebraic closure of \mathbb{Q}_p and \mathcal{O}_p its valuation ring. Given a ring A , we denote the set of nonzero elements by A^* and the set of units by A^\times . If K is a field, we denote its algebraic closure by K^{alg} . The set of restricted power series is denoted by

$$\mathbb{Z}_p\{\overline{X}\} = \left\{ \sum_I a_I \overline{X}^I \mid a_I \in \mathbb{Z}_p, v(a_I) \rightarrow \infty \right\}$$

where $\overline{X} = (X_1, \dots, X_n)$ and we use multi-index notation.

2 Weierstrass system and quantifier elimination

Definition 2.1. *A Weierstrass system over \mathbb{Z}_p is a family of rings $\mathbb{Z}_p[[X_1, \dots, X_n]]$, $n \in \mathbb{N}$, such that for all n , the following conditions hold:*

1. $\mathbb{Z}[\overline{X}] \subseteq \mathbb{Z}_p[[\overline{X}]] \subseteq \mathbb{Z}_p\{\overline{X}\};$
2. For all permutations σ of $\{1, \dots, n\}$, if $f(\overline{X}) \in \mathbb{Z}_p[[\overline{X}]]$, then $f(X_{\sigma(1)}, \dots, X_{\sigma(n)}) \in \mathbb{Z}_p[[\overline{X}]];$
3. If $f \in \mathbb{Z}_p[[\overline{X}]]$ has an inverse g in $\mathbb{Z}_p\{\overline{X}\}$, then $g \in \mathbb{Z}_p[[\overline{X}]];$
4. Let $k \in \mathbb{Z}$. If $f \in \mathbb{Z}_p[[\overline{X}]]$ is divisible by k in $\mathbb{Z}_p\{\overline{X}\}$, then $f/k \in \mathbb{Z}_p[[\overline{X}]];$
5. (Weierstrass division) If $f \in \mathbb{Z}_p[[X_1, \dots, X_{n+1}]]$ and f is regular of order d in X_{n+1} , then, for all $g \in \mathbb{Z}_p[[X_1, \dots, X_{n+1}]]$, there are $A_0, \dots, A_{d-1} \in \mathbb{Z}_p[[\overline{X}']]$ (where $\overline{X}' = (X_1, \dots, X_n)$) and $Q \in \mathbb{Z}_p[[\overline{X}]]$ such that

$$g(\overline{X}) = Q(\overline{X}) \cdot f(\overline{X}) + \left(X_{n+1}^{d-1} A_{d-1}(\overline{X}') + \dots + A_0(\overline{X}') \right).$$

Let $\mathcal{L}_{Mac} = (+, \cdot, 0, 1, P_n; n \in \mathbb{N})$ be the Macintyre's language for p -adically closed fields i.e. $+, \cdot, 0, 1$ are interpreted in \mathbb{Z}_p by the natural operations and P_n is a unary predicate for the set of n th powers i.e.

$$\mathbb{Z}_p \models P_n(x) \text{ iff } \exists y \in \mathbb{Z}_p \ x = y^n.$$

Fix a Weierstrass system $W = (\mathbb{Z}_p[[X_1, \dots, X_n]])_{n \in \mathbb{N}}$. Let \mathcal{L}_W be the extension of the language \mathcal{L}_{Mac} by function symbols f for each $f \in \mathbb{Z}_p[[X_1, \dots, X_n]]$ and \mathcal{L}_W^D be the expansion of \mathcal{L}_W by a division symbol D interpreted in \mathbb{Z}_p by:

$$D(x, y) = \begin{cases} x/y & \text{if } v(x) \geq v(y) \text{ and } y \neq 0 \\ 0 & \text{otherwise.} \end{cases}$$

Let $\mathbb{Z}_{p,W}$ (resp. $\mathbb{Z}_{p,W}^D$) be the structure with underlying set \mathbb{Z}_p and natural interpretations for the symbol of \mathcal{L}_W (resp. \mathcal{L}_W^D). Then, it follows from the proof of the quantifier elimination for p -adic subanalytic sets (see [2]) that

Proposition 2.2. *The theory of $\mathbb{Z}_{p,W}^D$ admits elimination of quantifiers.*

Note that the graph of the function D is strongly definable in \mathcal{L}_W . So, as an immediate corollary of the above proposition, we have

Corollary 2.3. *The theory of $\mathbb{Z}_{p,W}$ is strongly model-complete.*

3 Weierstrass system generated by a set of restricted analytic functions

Let F be a family of restricted analytic functions. As before, we denote by \mathcal{L}_F the expansion of the language \mathcal{L}_{Mac} by the elements of F . We will prove that under the condition that the set of \mathcal{L}_F -terms is closed under derivation

and *decomposition functions* (to be defined later), the theory $\mathbb{Z}_{p,F}$ is strongly model-complete.

Let W be any Weierstrass system which contains F . Then the theory of \mathbb{Z}_p eliminates the quantifiers in the language \mathcal{L}_W^D . In particular, if the functions in W are \mathcal{L}_F -existentially definable, we are done. In this section, we will define a Weierstrass system W_F such that any function in W_F is constructible from the data set F i.e. for all $f \in W_F$, there exists a finite collection of functions $f_1, \dots, f_k \in F$ from which one can construct f using polynomial combinations, Weierstrass divisions, permutations of the variables and inverses. We will see in the next section that under the above assumptions on F , any function in W_F is actually existentially definable.

We define *the Weierstrass system generated by the \mathcal{L}_F -terms* by:

For each n , let $W_{F,n}^{(0)}$ be the set of \mathcal{L}_F -terms with n variables. We define $W_{F,n}^{(m+1)}$ by induction on m . Assume that we have defined $W_{F,n}^{(k)}$ for each $n \in \mathbb{N}$ and for each $k \leq m$. Then, $W_{F,n}^{(m+1)}$ is the ring generated by:

- (a) $W_{F,n}^{(m)} \subset W_{F,n}^{(m+1)}$;
- (b) For all $f \in W_{F,n}^{(m)}$, for all permutations σ , $f(X_{\sigma(1)}, \dots, X_{\sigma(n)}) \in W_{F,n}^{(m+1)}$;
- (c) For all $f \in W_{F,n}^{(m)}$, if f is invertible in $\mathbb{Z}_p\{\overline{X}\}$, then $f^{-1} \in W_{F,n}^{(m+1)}$;
- (d) For all $f \in W_{F,n}^{(m)}$ and for all $k \in \mathbb{Z}$, if f is divisible by k in $\mathbb{Z}_p\{\overline{X}\}$, then $f/k \in W_{F,n}^{(m+1)}$;
- (e) For each $f \in W_{F,n+1}^{(m)}$ of order d in X_{n+1} , for each $g \in W_{F,n+1}^{(m)}$, the functions $A_0, \dots, A_{d-1} \in \mathbb{Z}_p\{X_1, \dots, X_n\}$ and $Q \in \mathbb{Z}_p\{X_1, \dots, X_{n+1}\}$ given by the Weierstrass division and their partial derivatives belong to $W_{F,n}^{(m+1)}$ and $W_{F,n+1}^{(m+1)}$ respectively.

Let $W_{F,n} := \bigcup_m W_{F,n}^{(m)}$. It is clear that these sets determine a Weierstrass system over \mathbb{Z}_p . We denote this system by W_F . Then, by proposition 2.2, the theory of \mathbb{Z}_p admits elimination of quantifiers in $\mathcal{L}_{W_F}^D$. We will show that each function of W_F is strongly definable in \mathcal{L}_F (under extra assumptions on F).

Remark. Let W be a Weierstrass system. Then, by closure under Weierstrass division, it follows that W is closed under derivation. Furthermore, if $W_F^{(0)}$ is closed under derivation then $W_F^{(m)} := \bigcup_n W_{F,n}^{(m)}$ is also closed under derivation for all m .

Note that by definition, for all $f \in W_{F,n}^{(m+1)}$, there exist $g_1, \dots, g_k \in W_{F,n+1}^{(m)}$ such that f is obtained from g_1, \dots, g_k using the above operations (a)-(e) and polynomial combinations. We denote this property by $f \in \langle g_1, \dots, g_k \rangle$.

We denote $f \in \langle f_1, \dots, f_k \rangle^*$ if we have a family of functions $f_{i,j}$ ($1 \leq i \leq k$, $1 \leq j \leq n$) such that

- $f \in W_F^{(m+n)}$, $f_{i,j} \in W_F^{(m+n-j)}$ for all i, j ;
- $f_{1,n} = f_1, \dots, f_{k,n} = f_k$;
- $f \in \langle f_{1,1}, \dots, f_{k,1} \rangle$ and $f_{ij} \in \langle f_{1,j+1}, \dots, f_{k,j+1} \rangle$ for all i, j .

It should be clear that by induction one can find for each $f \in W_F$ a finite collection of \mathcal{L}_F -terms f_1, \dots, f_d such that $f \in \langle f_1, \dots, f_d \rangle^*$. Furthermore,

Lemma 3.1. *Let $\Psi(\overline{X}) \equiv \exists Y_1, \dots, Y_n \phi(\overline{X}, \overline{Y})$ be a \mathcal{L}_F -formula where ϕ is quantifier-free. Then, there exists ϕ' a quantifier-free $\mathcal{L}_{W_F}^D$ -formula such that*

$$\mathbb{Z}_p \models \forall \overline{X} \left(\Psi(\overline{X}) \leftrightarrow \exists Z_1, \dots, Z_{n-1} \phi'(\overline{X}, \overline{Z}) \right).$$

Furthermore, for any subterm f in ϕ' (not involving D), there exists a subterm g in ϕ and P_1, \dots, P_m polynomials with coefficients in \mathbb{Z} such that $f \in \langle g, P_1, \dots, P_m \rangle^*$

This follows immediately from the proof of proposition 2.2. And, by induction, there exists a quantifier-free $\mathcal{L}_{W_F}^D$ -formula $\varphi(\overline{X})$ equivalent to Ψ such that for any term f in φ , $f \in \langle g_1, \dots, g_l, P_1, \dots, P_s \rangle^*$ where g_1, \dots, g_l are the \mathcal{L}_F -subterms in Ψ and P_1, \dots, P_s are polynomials with coefficients in \mathbb{Z} .

4 Decomposition functions and definability of finite algebraic extensions

Let F be a family of restricted analytic functions and W_F be the Weierstrass system generated by the \mathcal{L}_F -terms. We want to prove that any function of W_F is \mathcal{L}_F -existentially definable. Let $f \in W_F^{(m+1)}$. Then there are $g_1, \dots, g_k \in W_F^{(m)}$ such that $f \in \langle g_1, \dots, g_k \rangle$. Assume that each function g_i is existentially definable. Then so is f if it is constructed from g_1, \dots, g_k using the operations (a)-(d) and polynomial combinations. However, it is not clear whether it is also the case when f is obtained using Weierstrass division. In general, we couldn't conclude that this is the case. So, we will add extra-conditions on F so that the functions involved in the Weierstrass division are existentially definable from the data set. First, we illustrate the main idea of the existential definition on a simple example:

Let f be a \mathcal{L}_F -term of order d in X_{n+1} . Then, by the Weierstrass preparation theorem, there are $A_0, \dots, A_{d-1} \in W_{F,n}^{(1)}$ and a unit $U \in W_{F,n+1}^{(1)}$ such that:

$$f(X_1, \dots, X_{n+1}) = \left[X_{n+1}^d + A_{d-1}(\overline{X'}) X_{n+1}^{d-1} + \dots + A_0(\overline{X'}) \right] \cdot U(\overline{X}),$$

where $\overline{X'} = (X_1, \dots, X_n)$. We want to give an existential definition of the functions A_0, \dots, A_{d-1}, U . Fix $\overline{x'} = (x_1, \dots, x_n) \in \mathbb{Z}_p^n$. It is rather clear that $U(\overline{x'}, X)$ is strongly definable in terms of f and $A_0(\overline{x'}), \dots, A_{d-1}(\overline{x'})$. We will give the explicit definition of the graph of U later and focus now on the definition of the coefficients A_i .

Let $\alpha_1, \dots, \alpha_d$ be the roots of $P(X) := \sum A_i(\overline{x'})X^i + X^d$ in \mathbb{Q}_p^{alg} . Note that these are exactly the roots of $f(\overline{x'}, X)$ in \mathbb{Q}_p^{alg} with nonnegative valuation. Then, the coefficients $A_i(\overline{x'})$ are uniquely determined by $\alpha_1, \dots, \alpha_d$. For instance, if the roots are nonsingular (i.e. if $\alpha_i \neq \alpha_j$ for all $i \neq j$), the coefficients $A_i(\overline{x'})$ are uniquely determined by the system:

$$T(\overline{\alpha}, A_0(\overline{x'}), \dots, A_{d-1}(\overline{x'})) \equiv \begin{pmatrix} 1 & \alpha_1 & \dots & \alpha_1^{d-1} \\ \vdots & \vdots & & \vdots \\ 1 & \alpha_d & \dots & \alpha_d^{d-1} \end{pmatrix} \cdot \begin{pmatrix} A_0(\overline{x'}) \\ \vdots \\ A_{d-1}(\overline{x'}) \end{pmatrix} = \begin{pmatrix} \alpha_1^d \\ \vdots \\ \alpha_d^d \end{pmatrix}.$$

Other similar systems determine the coefficients in the case where the roots are singular. The above relation leads to an existential formula which determines the graphs of the functions A_i : $(\overline{x'}, \overline{a}) \in \text{Graph}(A_0, \dots, A_{d-1})$ iff the formula

$$\Psi(\overline{x'}, \overline{a}) \equiv \exists \overline{\alpha} \in \mathbb{Q}_p^{alg} \bigwedge_i f(\overline{x'}, \alpha_i) = 0 \wedge \left(\bigwedge_{i \neq j} \alpha_i \neq \alpha_j \wedge \bigwedge_i v(\alpha_i) \geq 0 \wedge T(\overline{\alpha}, \overline{a}) \right) \vee [\dots]$$

is satisfied in \mathbb{Z}_p , where $[\dots]$ holds for the disjunction of the systems determining $A_0(\overline{x'}), \dots, A_{d-1}(\overline{x'})$ in all possible singular cases. However, the existential quantifiers in this formula quantify over elements in \mathbb{Q}_p^{alg} (the α_i 's). Actually, using properties of finite extension of \mathbb{Q}_p we can quantify over a finite algebraic extension:

It follows from Krasner's lemma that the p -adic field \mathbb{Q}_p has finitely many algebraic extensions of a given degree (which can be assumed generated by elements algebraic over \mathbb{Q}). So, we can construct a sequence of finite algebraic extensions $K_1 \subseteq K_2 \subseteq \dots$ such that:

- K_n is the splitting field of $Q_n(X)$ polynomial of degree N_n with coefficients in \mathbb{Q} ;
- $K_n = \mathbb{Q}_p(\beta_n)$ for all β_n root of Q_n ;
- any extension of degree n is contained in K_n and its valuation ring is contained in $V_n := \mathbb{Z}_p[\beta_n]$.

Let us remark that for all $\overline{x'} \in \mathbb{Z}_p^n$, $\alpha_1, \dots, \alpha_d \in V_d$. So, in the above formula Ψ , we can quantify over V_d instead of \mathbb{Q}_p^{alg} .

Let $f \in F$. Then, f defines an analytic function on V_d . So, we can consider the structure $(V_d, +, \cdot, 0, 1, P_n, f; n \in \mathbb{N}, f \in F)$. If this structure

is existentially definable in $\mathbb{Z}_{p,F}$ then the above formula Ψ can be translated in \mathbb{Z}_p and we are done.

It is well known that the structure of ring is definable but this may not be the case for the elements of F . We will extend F by a family of functions \tilde{F} so that the structure $(V_d, +, \cdot, 0, 1, P_n, f; n \in \mathbb{N}, f \in \tilde{F})$ is existentially definable in $\mathbb{Z}_{p,\tilde{F}}$.

For this, it is sufficient to describe the decomposition of f in the basis of V_d over \mathbb{Z}_p . Fix $f \in F$ and $y = \sum y_i \beta_d^i \in V_d^k$ (where $y_i \in \mathbb{Z}_p^k$). We decompose $f(y)$ in the basis of V_d over \mathbb{Z}_p :

$$f(y) = f\left(\sum y_i \beta_d^i\right) = c_{0,f,d}(\bar{y}) + c_{1,f,d}(\bar{y})\beta_d + \cdots + c_{N_d-1,f,d}(\bar{y})\beta_d^{N_d-1},$$

where $\bar{y} = (y_1, \dots, y_{N_d})$. It determines functions $c_{i,f,d} \in \mathbb{Z}_p\{X_1, \dots, X_{N_d}\}$. We call these functions *the decomposition functions of f in K_d* . Note that these functions are independent of the choice of β_d . Indeed, for all σ in the Galois group of K_d over \mathbb{Q}_p (denoted by $\text{Gal}(K_d/\mathbb{Q}_p)$),

$$f(y^\sigma) = f\left(\sum y_i \beta_d^{\sigma^i}\right) = c_{0,f,d}(\bar{y}) + c_{1,f,d}(\bar{y})\beta_d^\sigma + \cdots + c_{N_d-1,f,d}(\bar{y})\beta_d^{\sigma^{N_d-1}}, (*)$$

by continuity of σ . Let $\tilde{F} := F \cup \{c_{i,f,d} \mid f \in F, d \in \mathbb{N} \text{ and } i < N_d\}$. Then, by definition,

Lemma 4.1. *For all d , the structure $(V_d, +, \cdot, 0, 1, P_n, f; n \in \mathbb{N}, f \in F)$ is existentially definable in $\mathbb{Z}_{p,\tilde{F}}$.*

At this point, one may expect that we will need to add further decomposition functions so that the structure $(V_d, +, \cdot, 0, 1, P_n, f; n \in \mathbb{N}, f \in \tilde{F})$ is also definable. However this is not the necessary. Indeed, let us remark that the $c_{i,f,d}(\bar{y})$ are linear combinations of the $f(y^\sigma)$: by (*),

$$\begin{pmatrix} c_{0,f,d}(\bar{y}) \\ \vdots \\ c_{N_d-1,f,d}(\bar{y}) \end{pmatrix} = V^{-1} \begin{pmatrix} f(y^{\sigma^1}) \\ \vdots \\ f(y^{\sigma^{N_d}}) \end{pmatrix},$$

where V is the Vandermonde matrix of the roots of Q_d and σ_i are the elements of $\text{Gal}(K_d/\mathbb{Q}_p)$. So, as power series,

$$c_{i,f,d}(\bar{y}) = \sum a_i \beta_d^i f\left(\sum R_i(\bar{y}) \beta_d^i\right),$$

where $a_i \in \mathbb{Q} \cap \mathbb{Z}_p$ and R_i is a polynomial with coefficients in $\mathbb{Z}_p \cap \mathbb{Q}$. Therefore, the above relation holds for all $\bar{y} \in V_l^{kN_d}$. So,

Proposition 4.2. *For all d , the structure $(V_d, +, \cdot, 0, 1, P_n, f; n \in \mathbb{N}, f \in \tilde{F})$ is existentially definable in $\mathbb{Z}_{p,\tilde{F}}$.*

Finally note that if the set of \mathcal{L}_F -terms is closed under derivation, so is the set of $\mathcal{L}_{\tilde{F}}$ -terms. This follows immediately from the above equalities.

5 Strong model-completeness

First, let us describe the existential definitions of the functions in W_F .

Proposition 5.1. *Let F be a family of functions in $\mathbb{Z}_p\{\overline{X}\}$. Assume that the set of \mathcal{L}_F -terms is closed under derivation. Let \tilde{F} be the extension of F by the decomposition functions in K_d of each $f \in F$ (for all $d \in \mathbb{N}$). Let $g \in W_{\tilde{F}}$. Then g is strongly definable in $\mathcal{L}_{\tilde{F}}$. Furthermore, for all d , the structure $(V_d, +, \cdot, 0, 1, g)$ is strongly definable in \mathbb{Z}_p, \tilde{F} .*

Given a function $f \in \mathbb{Z}_p\{X_1, \dots, X_n\}$, we denote the set $\left\{ \frac{\partial^k f}{\partial X_i^k}; 1 \leq i \leq n, k \in \mathbb{N} \right\}$ by $[f]$.

Proof. The proof is very similar to the corresponding results in [7]. The definitions given in the below claims are roughly the same that in the real case.

Let us recall that for all $f \in W_{\tilde{F},n}^{(m+1)}$, there exist $g_1, \dots, g_k \in W_{\tilde{F}}^{(m)}$ such that $f \in \langle g_1, \dots, g_k \rangle$. So, it is sufficient to prove by induction on m that

1. For all $f \in W_{\tilde{F},n}^{(m+1)}$, f and its derivatives are strongly definable in terms of functions in $W_{\tilde{F},n+1}^{(m)}$ (and their derivatives);
2. The definitions remain true uniformly over the algebraic extensions V_d i.e. the graphs of the function $f : V_d^k \rightarrow V_d$ and of its derivatives are strongly definable in terms of functions in $W_{\tilde{F},n+1}^{(m)}$ (and their derivatives).

By definition of the language $\mathcal{L}_{\tilde{F}}$ and by proposition 4.2, it is clear that the extensions of the functions in $W_{\tilde{F},n}^{(0)}$ to V_d are definable. And so are the graphs of their derivatives as the set of $\mathcal{L}_{\tilde{F}}$ -terms is closed under derivation. So, we assume by induction that the graph of the extension to V_d of any function in $W_{\tilde{F},n}^{(k)}$ (or one of its derivative) is strongly definable in our structure for all d , for all n and for all $k \leq m$.

Let $f \in W_{\tilde{F},n}^{(m+1)}$. Then, $f = P(f_1, \dots, f_k)$ where $P \in \mathbb{Z}[\overline{Y}]$ and $f_1, \dots, f_k \in W_{\tilde{F},n}^{(m+1)}$ are functions of the type (a)-(e) in the definition of Weierstrass system generated by the \mathcal{L}_F -terms. If the functions f_1, \dots, f_k satisfy properties 1. and 2., then f also satisfies these properties. Indeed, the graph of f is strongly definable in terms of f_1, \dots, f_k as (\overline{x}, y) is a point of the graph of f as functions from \mathbb{Z}_p to itself (or as function from V_d to itself if the below formula is satisfied in V_d) iff

$$\mathbb{Z}_p \models \exists t_1 \dots \exists t_k \bigwedge t_i = f_i(\overline{x}) \wedge y = P(t_1, \dots, t_k).$$

Similarly for the derivatives of f . So, we can assume that f is a function of the type (a)-(e).

The cases where f is obtained as the division of a function $g \in W_{\tilde{F},n}^{(m)}$ by an integer by k or is a function g in $W_{\tilde{F},n}^{(m)}$ (i.e. $k = 1$) are obvious: $(\bar{x}, y) \in \text{Graph}(f)$ iff

$$\mathbb{Z}_p \models ky = g(\bar{x}).$$

If $f(\bar{X}) = g(X_{\sigma(1)}, \dots, X_{\sigma(n)})$ where σ is a permutation of $\{1, \dots, n\}$ then the tuple (\bar{x}, y) belongs to the graph of f iff

$$\mathbb{Z}_p \models \exists \bar{t} \bigwedge_i t_i = x_{\sigma(i)} \wedge y = g(\bar{t}).$$

If f is the inverse of a function g , then (\bar{x}, y) belongs to the graph of f iff

$$\mathbb{Z}_p \models yg(\bar{x}) = 1.$$

Therefore, in these cases (a)-(d), both the graphs of f , of its derivatives and their extensions to V_d are strongly definable in terms of $[g]$. So, we are reduced to the case (e):

Let $f, g \in W_{\tilde{F},n+1}^{(m)}$ where f has order d in $Y = X_{n+1}$. Then, there are $A_0, \dots, A_{d-1} \in W_{\tilde{F},n}^{(m+1)}$ and $Q \in W_{\tilde{F},n+1}^{(m+1)}$ such that

$$g = Qf + (A_{d-1}Y^{d-1} + \dots + A_1Y + A_0).$$

We have to prove that A_0, \dots, A_{d-1}, Q (and their derivatives) are strongly definable in \mathbb{Z}_p and that the definitions work uniformly over the algebraic extensions V_d .

Claim 1. A_0, \dots, A_{d-1} are strongly definable in terms of $[f, g]$.

Proof. Fix $\bar{x} \in \mathbb{Z}_p^n$. Let $\alpha_1, \dots, \alpha_d$ be the roots of $f(\bar{x}, Y)$ in V_d (we take in account multiplicities). Then, $A_0(\bar{x}), \dots, A_{d-1}(\bar{x})$ are uniquely determined by these roots. Indeed, first assume that the roots are distinct. In this case, $A_0(\bar{x}), \dots, A_{d-1}(\bar{x})$ are determined by the relations:

$$\alpha_i \neq \alpha_j \text{ for all } i, j$$

$$f(\bar{x}, \alpha_i) = 0 \text{ for all } i$$

$$\begin{pmatrix} 1 & \alpha_1 & \dots & \alpha_1^{d-1} \\ \vdots & \vdots & & \vdots \\ 1 & \alpha_d & \dots & \alpha_d^{d-1} \end{pmatrix} \begin{pmatrix} A_0(\bar{x}) \\ \vdots \\ A_{d-1}(\bar{x}) \end{pmatrix} = \begin{pmatrix} g(\bar{x}, \alpha_1) \\ \vdots \\ g(\bar{x}, \alpha_d) \end{pmatrix}.$$

If $f(\bar{x}, Y)$ admits singular roots, say $\alpha_1 = \alpha_2$ and $\alpha_i \neq \alpha_j$ for all $i \neq j$, $i, j \neq 2$ for instance, then we replace the d equations $f(\bar{x}, \alpha_1) = \dots =$

$f(\bar{x}, \alpha_d) = 0$ by $f(\bar{x}, \alpha_1) = \frac{\partial f}{\partial Y}(\bar{x}, \alpha_1) = f(\bar{x}, \alpha_3) = \dots = f(\bar{x}, \alpha_d) = 0$. The functions A_i are determined in this case by the relations:

$$\alpha_i \neq \alpha_j \text{ for all } i \neq j, j \neq 2$$

$$f(\bar{x}, \alpha_i) = 0 \text{ for all } i \neq 2$$

$$\frac{\partial f}{\partial Y}(\bar{x}, \alpha_1) = 0$$

$$\begin{pmatrix} 1 & \alpha_1 & \dots & \alpha_1^{d-1} \\ 0 & 1 & \dots & (d-1)\alpha_1^{d-2} \\ 1 & \alpha_3 & \dots & \alpha_3^{d-1} \\ \vdots & \vdots & & \vdots \\ 1 & \alpha_d & \dots & \alpha_d^{d-1} \end{pmatrix} \begin{pmatrix} A_0(\bar{x}) \\ A_1(\bar{x}) \\ A_2(\bar{x}) \\ \vdots \\ A_{d-1}(\bar{x}) \end{pmatrix} = \begin{pmatrix} g(\bar{x}, \alpha_1) \\ \frac{\partial g}{\partial Y}(\bar{x}, \alpha_1) \\ g(\bar{x}, \alpha_3) \\ \vdots \\ g(\bar{x}, \alpha_d) \end{pmatrix}.$$

For each configuration of multiplicities of the roots of $f(\bar{x}, Y)$, the coefficients A_i are completely determined by a system like above. We proceed to a disjunction over all possible cases to define the graphs of A_0, \dots, A_{d-1} on \mathbb{Z}_p^n .

Let $\Psi(\bar{x}, A_0(\bar{x}), \dots, A_{d-1}(\bar{x}), \bar{\alpha})$ be the disjunction of all possible system like above. Then, the following formula gives an existential definition of the graphs of A_0, \dots, A_{d-1} :

$$\exists \alpha_1 \dots \alpha_d \in V_d \Psi(\bar{x}, A_0(\bar{x}), \dots, A_{d-1}(\bar{x}), \bar{\alpha}).$$

Let us remark that the above definition is an existential definitions where we quantify over V_d . We interpret this formulas in \mathbb{Z}_p . So, formally, the α_i 's are replaced by tuples. The additions, multiplications (in V_d in Ψ) are replaced by their interpretation in \mathbb{Z}_p . Similarly, the functions f, g , their derivatives are also replaced by their interpretations in \mathbb{Z}_p (which exists by inductive hypothesis).

Note also that the α_i 's are only unique up to permutation. It means that so far, we have only existentially defined the graphs of the A_i 's. We transform this existential definition into a strong existential formula using [1]. In this paper, J. Denef gives a formula of definable selection for finite sets i.e. a quantifier-free formula $D(x, X)$ (where X is a new predicate) such that for all $X(\bar{v})$ a predicate corresponding to a finite set in \mathbb{Q}_p :

$$\begin{aligned} \mathbb{Q}_p \models \exists v_1, \dots, v_s \quad & \left[\bigwedge_i X(v_i) \wedge \bigwedge_{i,j} v_i \neq v_j \right] \\ & \rightarrow \exists ! v_1, \dots \exists ! v_s \left[\bigwedge_i X(v_i) \wedge \bigwedge_i D(v_i, X) \wedge \bigwedge_{i,j} v_i \neq v_j \right]. \end{aligned}$$

We use this formula with X equals to the set $\{\alpha_1, \dots, \alpha_d\}$ (interpreted in \mathbb{Z}_p) to get a strong definition of the graphs of the A_i 's. \square

Note that the above formula works uniformly over the algebraic extensions. Therefore, the graphs of the A'_i 's as functions from V_d^n to V_d are also strongly definable.

Claim 2. *Q and its derivatives (with respect to Y) are strongly definable in terms of $[f, g], A_0, \dots, A_{d-1}$.*

Claim 3. *For all I, j , $\frac{\partial^I A_0}{\partial \bar{X}^I}, \dots, \frac{\partial^I A_{d-1}}{\partial \bar{X}^I}$ and $\frac{\partial^I}{\partial \bar{X}^I} \frac{\partial^j Q}{\partial Y^j}$ are strongly definable in terms of $[f, g]$.*

The definitions are the same that in [7] lemma 3.4 and proposition 3.8 respectively. Again, it leads to existential definitions where the quantifiers are over V_d and we have to interpret these formulas in \mathbb{Z}_p . Note that the definitions also work uniformly over finite algebraic extensions.

This proves that A_0, \dots, A_{d-1}, Q and their derivatives are strongly definable functions in terms of functions in $W_{\tilde{F}, n+1}^{(m)}$ and therefore completes the proof of the proposition. \square

The first main theorem follows immediately from propositions 2.2 and 5.1

Theorem 5.2. *Let F be a family of restricted analytic functions. Assume that the set of \mathcal{L}_F -terms is closed under derivation. Let \tilde{F} be the extension of F by the decomposition functions of each $f \in F$. Then, $\mathbb{Z}_{p, \tilde{F}}$ is strongly model-complete in $\mathcal{L}_{\tilde{F}}$.*

6 Effective Weierstrass system

Let F be a family of restricted analytic functions. We assume that the set of \mathcal{L}_F -terms is closed under derivation. We also assume that this family is an *effective family of restricted analytic functions* i.e. that F is recursively enumerable and that, for all I , there exists some algorithm \mathcal{D} which takes for entries functions f in F and returns a \mathcal{L}_F -term g such that $\frac{\partial^I f}{\partial \bar{X}^I} = g$.

We want to prove now an effective version of theorem 5.2 i.e. prove that there is an algorithm which takes for entry a $\mathcal{L}_{\tilde{F}}$ -formula $\Psi(\bar{x})$ and returns a strong existential formula $\varphi(\bar{x})$ equivalent to $\Psi(\bar{x})$.

First, let us remark that our strong definitions of the functions in W_F (proposition 5.1) are effective. So, we have an explicit description of φ modulo an effective version of proposition 2.2.

This proposition relies on the elimination of quantifiers in [2]. An inspection of the proof of the main theorem [2] shows that it is effective except for the use of lemma 1.4. Let us recall this lemma:

Lemma 6.1 (Lemma 1.4 in [2]). *Let $f(\overline{X}, \overline{Y}) = \sum a_I(\overline{Y}) \overline{X}^I \in \mathbb{Z}_p\{\overline{X}, \overline{Y}\}$. Then, there is $d \in \mathbb{N}$ such that, for all I with $|I| \geq d$ (where $|I| = i_1 + \dots + i_m$),*

$$a_I(\overline{Y}) = \sum_{|J| < d} b_{IJ}(\overline{Y}) a_J(\overline{Y}),$$

where $b_{IJ}(\overline{Y}) \in \mathbb{Z}_p\{\overline{Y}\}$ with $\|b_{IJ}(\overline{Y})\| < 1$ (where $\|\sum c_I \overline{Y}^I\| = \min\{v(c_I)\}$).

The existence of d follows from the Noetherian property of the ring $\mathbb{Z}_p\{\overline{Y}\}$. In general, we cannot expect that this integer d is computable.

Definition 6.2. *Let $f \in \mathbb{Z}_p\{X_1, \dots, X_n, \overline{Y}\}$. We say that f has an effective n -Weierstrass bound if one can compute $d(f)$ an upper bound for the smallest integer d like in lemma 6.1.*

A Weierstrass system for which there is an algorithm which compute $d(f)$ for each function f of the system is called an *effective Weierstrass system*.

Definition 6.3. *A Weierstrass system $(\mathbb{Z}_p\llbracket X_1, \dots, X_n \rrbracket)_{n \in \mathbb{N}}$ is called effective if there exists an algorithm which takes for entries functions f of the system and returns an integer $d(f)$ such that, for all I with $|I| \geq d(f)$,*

$$a_I(\overline{Y}) = \sum_{|J| < d(f)} b_{IJ}(\overline{Y}) a_J(\overline{Y}),$$

where $f(\overline{X}, \overline{Y}) = \sum a_I(\overline{Y}) \overline{X}^I$ and $b_{IJ} \in \mathbb{Z}_p\{\overline{Y}\}$ with $\|b_{IJ}\| < 1$.

So if the Weierstrass system generated by the $\mathcal{L}_{\tilde{F}}$ -terms is effective then the strong model-completeness in theorem 5.2 is effective. The second main theorem says that under the assumptions of theorem 5.2 and assuming that we can compute (a generalisation of) the above number $d(f)$ for any $\mathcal{L}_{\tilde{F}}$ -term, the Weierstrass system $W_{\tilde{F}}$ is effective.

We will now assume that for all \mathcal{L}_F -term f , f has an effective 1-Weierstrass bound. First, we show that the integer $d(f)$ can be computed for each term in our language (i.e. each \mathcal{L}_F -term with $n + m$ variables has an effective n -Weierstrass bound). This property was already observed by A. Macintyre in [4].

Proposition 6.4. *Let F be any effective family of restricted analytic functions. Assume that each \mathcal{L}_F -term has an effective 1-Weierstrass bound. Then, there exists a computable function D from the set of \mathcal{L}_F -terms to \mathbb{N} such that for all \mathcal{L}_F -term $f(\overline{X}, \overline{Y})$, if d is the smallest integer like in lemma 6.1, then $d \leq D(f)$.*

Proof. Let $f(\overline{X}, \overline{Y}) = \sum a_I(\overline{Y}) \overline{X}^I$. Let d be the smallest integer like in lemma 6.1. Then, for all $\overline{y} \in \mathbb{Z}_p^m$, one of the following formulas is satisfied in \mathbb{Z}_p :

$$Z(\overline{Y}) \equiv \bigwedge_{|J| < d} a_J(\overline{Y}) = 0,$$

or, for some $|I| < d$,

$$\mu_{I,f}(\bar{Y}) \equiv \bigwedge_{J < I} v(a_I(\bar{Y})) \leq v(a_J(\bar{Y})) \wedge \bigwedge_{I < J, |J| < d} v(a_I(\bar{Y})) < v(a_J(\bar{Y})).$$

If $Z(\bar{y})$ is satisfied for all $\bar{y} \in \mathbb{Z}_p^m$, we can take $D(f) = 1$.

Fix $\bar{y} \in \mathbb{Z}_p^m$ and assume $\mu_{I,f}(\bar{y})$ holds where $I = (i_1, \dots, i_n)$ with $i_1 \neq 0$ (unless $Z(\bar{y})$ or $\mu_{(0, \dots, 0), f}(\bar{y})$ is satisfied, we can assume that this is the case). Then,

$$\begin{aligned} a_I^{-1}(\bar{y})f(\bar{X}, \bar{y}) &= \sum_{J < I} \left(a_J(\bar{y})/a_I(\bar{y}) \right) \bar{X}^J + \bar{X}^I + \sum_{I < J, |J| < d} \left(a_J(\bar{y})/a_I(\bar{y}) \right) \bar{X}^J \\ &\quad + \sum_{|K| \geq d} \left\{ \sum_{J < I} \left(a_J(\bar{y})/a_I(\bar{y}) \right) b_{KJ}(\bar{y}) + b_{KI}(\bar{y}) \right. \\ &\quad \left. + \sum_{I < J, |J| < d} \left(a_J(\bar{y})/a_I(\bar{y}) \right) b_{KJ}(\bar{y}) \right\} \bar{X}^K. \end{aligned}$$

We introduce new variables V_J and replace the quotients a_J/a_I by V_J or pV_J according if $J < I$ or $I < J$, for $|J| < d$. It defines a function:

$$\begin{aligned} \tilde{f}(\bar{X}, \bar{V}, \bar{Y}) &= \sum_{J < I} V_J \bar{X}^J + \bar{X}^I + \sum_{I < J, |J| < d} pV_J \bar{X}^J \\ &\quad + \sum_K \left(\sum_{J < I} V_J b_{KJ} + b_{KI} + \sum_{I < J, |J| < d} pV_J b_{KJ} \right) \bar{X}^K. \end{aligned}$$

Then, $f(\bar{X}, \bar{y}) = a_I(\bar{y})\tilde{f}(\bar{X}, \bar{v}, \bar{y})$ where $v_J = a_J(\bar{y})/a_I(\bar{y})$ or $a_J(\bar{y})/pa_I(\bar{y})$. And, if we proceed to change of variables

$$\begin{cases} X_i \longrightarrow Z_i - Z_n^{d^{n-i}} \text{ if } i < n \\ X_n \longrightarrow Z_n, \end{cases}$$

the function $\tilde{f}(\bar{Z}, \bar{v}, \bar{y})$ has order $S = i_n + i_{n-1}d + \dots + i_1d^{n-1}$ in Z_n . By the Weierstrass preparation theorem,

$$\tilde{f}(\bar{Z}, \bar{V}, \bar{y}) = \left(Z_n^S + A_{S-1}(Z_1, \dots, Z_{n-1}, \bar{V}, \bar{y})Z_n^{S-1} + \dots + A_0(Z_1, \dots, Z_{n-1}, \bar{V}, \bar{y}) \right) U(\bar{Z}, \bar{V}, \bar{y}).$$

And ,

$$f(\bar{Z}, \bar{y}) = a_I(\bar{y})\tilde{f}(\bar{Z}, \bar{v}, \bar{y}).$$

So, for any $z_1, \dots, z_{n-1} \in \mathbb{Z}_p$, $f(Z_n, \bar{z}', \bar{y})$ has exactly S roots (counting multiplicities) in \mathcal{O}_p . By Strassmann theorem, the integer $d(f)$ given by the 1-Weierstrass bound of f determines an effective upper bound of S and therefore of d (unless $\mu_{I,f}(\bar{y})$ holds with $I = (0, \dots, 0)$ for all \bar{y} , in which case, we can take $D(f) = 1$). Take $D(f) = d(f) + 1$ and it satisfies the property of the proposition. \square

So, we see that W_F is an effective Weierstrass system if and only if each function in W_F has a 1-Weierstrass bound. For this, by the proof of the proposition, it is sufficient to compute the following:

Let $f(X, \bar{Y}) \in W_F$. Then, it is equivalent to compute a bound to $D(f)$ like in the proposition or to compute a bound on the number of solutions in \mathcal{O}_p of $f(X, \bar{y}) = 0$ (whenever this number is finite) such that this bound does not depend on the parameter \bar{y} . Indeed, let $S(f)$ be such a bound. Then, if $S(f)$ is computable, f has an effective Weierstrass bound given by $S(f) + 1$.

Let f be a function in our Weierstrass system. Then, there are integers n and $m + 1$ such that $f \in W_{F,n}^{(m+1)}$. Also, f has an existential definition in terms of functions in $W_{F,n+1}^{(m)}$: there exist $g_1, \dots, g_k \in W_{F,n+1}^{(m)}$ such that $f \in \langle g_1, \dots, g_k \rangle$. Going down by induction, we may assume that the g_i 's are \mathcal{L}_F -terms. We will show that we can find effectively a uniform bound on the number of solutions in \mathcal{O}_p of $f(X, \bar{y}) = 0$ and that this bound can be expressed in terms of $d(g_1), \dots, d(g_k)$. So, assuming that $d(g_1), \dots, d(g_k)$ are computable, we will be able to compute $S(f)$.

The cases where f is obtained from a function g by inversion, permutation of the variables or division by an integer are rather easy. The main difficulty is the case where f is obtained using Weierstrass division. In this case, by the definitions given in the claims 1 to 3 in proposition 5.1, we see that zeros of such a function correspond to zeros of systems of n' equations in $W_{F,n'}^{(m)}$ (with t parameters).

We will now bound the number of solutions in $(\mathcal{O}_p^*)^n$ of a general system of n analytic functions with n variables (uniformly over parameters). For this, we will use results of tropical analytic geometry from [6].

7 Effective bound on the number of solutions in \mathcal{O}_p^* of some effective analytic system

First, we start this section by stating some results and definitions from [6] that will be used in our proofs. Let us remark that we do not state the definitions nor the results in full generality but we have restricted them in the case of our interest. In particular, the results hold if we replace \mathbb{Q}_p by any of its finite algebraic extension or by \mathbb{C}_p .

Let $P = \prod [r_i, \infty) \subset \mathbb{R}^n$ with $r_i \in \mathbb{Q}$. Then, $\mathbb{Z}_p \langle P \rangle$ denotes the set of power series in $\mathbb{Z}_p[[\bar{X}]]$ convergent on the product of balls with center 0 and radius p^{-r_i} i.e.

$$\mathbb{Z}_p \langle P \rangle = \left\{ \sum a_I \bar{X}^I \mid v(a_I) + \langle I, v(\bar{x}) \rangle \rightarrow \infty \forall \bar{x} \text{ such that } v(\bar{x}) \in P \right\},$$

(where $\langle \cdot, \cdot \rangle$ denotes the usual scalar product and the limit is taken over $|I| \rightarrow \infty$). For instance, if $P = \prod [0, \infty)^n$ then $\mathbb{Z}_p \langle P \rangle = \mathbb{Z}_p \{\bar{x}\}$.

Let $\bar{x} \in \mathbb{C}_p^n$. The *tropicalization* of \bar{x} , denoted by $\text{trop}(\bar{x})$, is the tuple formed by the valuations of the x_i 's:

$$\text{trop}(\bar{x}) = (v(x_1), \dots, v(x_n)).$$

Let $f \in \mathbb{Z}_p\langle P \rangle$ and $C \subseteq \bar{P} := \prod [r_i, \infty]$, we denote

$$V(f; C) = \{\bar{x} \in \mathbb{C}_p \mid \text{trop}(\bar{x}) \in C \text{ and } f(\bar{x}) = 0\}.$$

If $C = \bar{P}$, we denote the above set by $V(f)$.

We define the *tropicalization* of f as the closure of the set

$$\{\nu \in \bar{P} \mid \text{there exists } \bar{x} \in V(f) \text{ such that } \text{trop}(\bar{x}) = \nu\},$$

where the closure is taken in \bar{P} . We denote this set by $\text{Trop}(f, P)$ or by $\text{Trop}(f)$ when P is clear from the context.

$\text{Trop}(f)$ is actually completely determined by the coefficients of f : Let $f = \sum a_I \bar{X}^I \in K\langle P \rangle$. Fix $\nu \in P$. Let

$$\begin{aligned} \text{vert}_\nu(f) = \{ (I, v(a_I)) \mid v(a_I) + \langle I, \nu \rangle \leq \text{val}(a_{I'}) + \langle I', \nu \rangle \\ \text{for all monomials } a_{I'} \bar{X}^{I'} \text{ of } f \}. \end{aligned}$$

This is the set of points such that the linear functional $(\nu, 1)$ reaches its minimum. As $f \in \mathbb{Z}_p\langle P \rangle$, $v(a_I) + \langle I, \nu \rangle \rightarrow \infty$. So, $\text{vert}_\nu(f)$ is actually a finite set. Furthermore, it is proved in [6] that $\text{vert}_P(f) = \bigcup_{\nu \in P} \text{vert}_\nu(f)$ is finite.

We define the *initial form of f with respect to ν* to be

$$\text{in}_\nu(f) = \sum_{(I, v(a_I)) \in \text{vert}_\nu(f)} a_I \bar{X}^I \in \mathbb{Z}_p[\bar{X}].$$

Let us remark that

$$\text{vert}_\nu(f) = \{ (I, v(a_I)) \mid a_I \bar{X}^I \text{ is a monomial of } \text{in}_\nu(f) \}.$$

Let $f \in \mathbb{Z}_p\langle P \rangle$. Let $\bar{t} \in \mathbb{C}_p^n$ such that $f(\bar{t}) = 0$. By the ultrametric inequality, we have that for some $I, I' \in \mathbb{N}^n$ distinct, $v(a_I \bar{t}^I) = \text{val}(a_{I'} \bar{t}^{I'}) = \min_J \{ \text{val}(a_J \bar{t}^J) \}$. So, if $\nu = v(\bar{t}) \in \text{Trop}(f)$, $\text{in}_\nu(f)$ is not a monomial. A crucial result in [6] is that the converse is true:

Lemma 7.1 (lemma 8.4 in [6]). *Let $f \in \mathbb{Z}_p\langle P \rangle$ nonzero. Then,*

$$\text{Trop}(f) = \{ \nu \in \bar{P} \mid \text{in}_\nu(f) \text{ is not a monomial} \}.$$

So, $\text{Trop}(f)$ is determined by the $\text{in}_\nu(f)$ i.e. by the coefficients of f . $\text{Trop}(f) \cap \mathbb{R}^n$ is actually a very simple subset of \mathbb{R}^n : a polyhedral complex.

Definition 7.2. A polyhedral complex is a finite collection Π of polyhedra in \mathbb{R}^n (called faces or cells of Π) such that

- if $P, P' \in \Pi$, $P \cap P' \neq \emptyset$, then $P \cap P'$ is a face of P and a face of P' ;
- for all $P \in \Pi$ if F is a face of P then $F \in \Pi$.

The support of Π , denoted $|\Pi|$ is the set $\bigcup_{P \in \Pi} P$. The dimension of Π is the dimension of the highest dimensional cell of Π (the dimension of a polyhedron P is the dimension of the smallest affine subspace of \mathbb{R}^n containing P).

For $\nu \in \text{Trop}(f) \cap \mathbb{R}^n$, we define

$$\gamma_\nu = \{\nu' \in \text{Trop}(f) \cap \mathbb{R}^n \mid \text{vert}_{\nu'}(f) \supseteq \text{vert}_\nu(f)\}.$$

If $\text{Trop}(f)$ is non-empty, the collection $\{\gamma_\nu, \nu \in \text{Trop}(f) \cap \mathbb{R}^n\}$ is a polyhedral complex in \mathbb{R}^n of codimension at least 1 (i.e. all maximal cells have dimension at most $n - 1$). The support of this complex is exactly $\text{Trop}(f) \cap \mathbb{R}^n$. We will denote by $\text{Trop}(f) \cap \mathbb{R}^n$ the complex as well as its support.

Let $\pi : \mathbb{N}^n \times \mathbb{R} \rightarrow \mathbb{N}^n$ denote the projection on the n first coordinates. We define

$$\check{\gamma}_\nu = \pi(\text{conv}(\text{vert}_\nu(f))).$$

This is a bounded polyhedron. The *Newton complex* of f is the collection of polyhedra $\{\check{\gamma}_\nu \mid \nu \in P\}$. We denote by $\text{New}(f, P)$ this set or by $\text{New}(f)$ when P is clear from the context. In general this set is not a polyhedral complex: some face of a polyhedron in $\text{New}(f)$ may not belong to $\text{New}(f)$. Indeed, a face of a polyhedron $\check{\gamma}_\nu$ may correspond to the projection of a set $\text{conv}(\text{vert}_\nu(f))$ where $\nu \notin P$ (or f is not convergent at elements of tropicalization ν). It turns out that it is a polyhedral complex in the case where f is polynomial (in which case we consider the set of all $\check{\gamma}_\nu$ for $\nu \in \mathbb{R}^n$). The support of $\text{New}(f)$ is

$$|\text{New}(f)| = \text{conv}\{I \in \mathbb{N} \mid (I, \text{val}(a_I)) \in \text{vert}_\nu(f) \text{ for some } \nu \in \text{Trop}(f) \cap \mathbb{R}^n\}.$$

We will also denote this support by $\text{New}(f)$. The complexes $\text{New}(f)$ and $\text{Trop}(f) \cap \mathbb{R}^n$ are dual to each other in the following sense:

- Proposition 7.3** (J. Rabinoff [6]).
1. For all $\nu, \nu' \in \text{Trop}(f) \cap \mathbb{R}^n$, γ_ν is a face of $\gamma_{\nu'}$ iff $\check{\gamma}_{\nu'}$ is a face of $\check{\gamma}_\nu$.
 2. For all $\nu \in \text{Trop}(f) \cap \mathbb{R}^n$, γ_ν and $\check{\gamma}_\nu$ are orthogonal in the sense that the linear subspaces of \mathbb{R}^n associated to the affine spans of γ_ν and $\check{\gamma}_\nu$ are orthogonal. Furthermore, $\dim(\gamma_\nu) + \dim(\check{\gamma}_\nu) = \dim(\mathbb{R}^n)$.

The above proposition implies that we have one-to-one correspondence between cells of $\text{Trop}(f) \cap \mathbb{R}^n$ and positive dimensional polyhedra in $\text{New}(f)$.

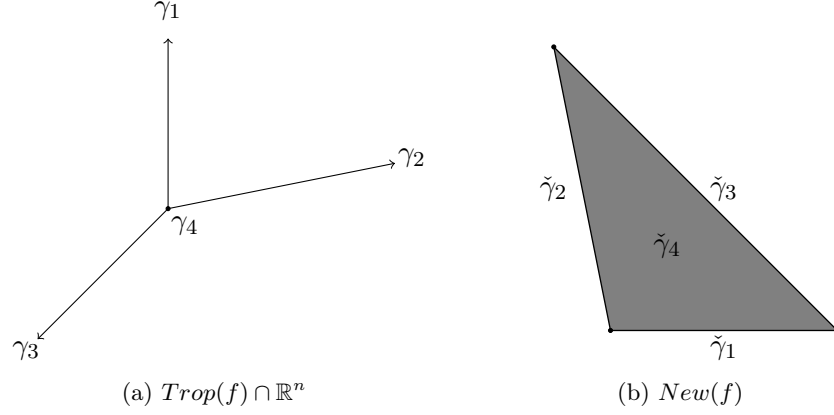


Figure 1: The tropicalization and Newton complex of $px + x^p + y^p$.

Example 7.1. Let $f(x, y) = px + x^p + y^p$. We have drawn the tropicalization and the Newton polygon of f in figure 1. Where in these figures, we take $P = (-\infty, +\infty)^2$ (with the obvious extensions of the definitions). If $P = [r, \infty) \times [s, \infty)$, then $Trop(f) \cap \mathbb{R}^n$ is the intersection between the set described in the above figure and P . $New(f)$ is the collection of all $\check{\gamma}_i$ such that $\gamma_i \cap P$ has the same dimension that γ_i .

One of the main result of [6] is a generalisation of the classical result on Newton polygons for power series in \mathbb{Z}_p . It relates the number of solutions with a given valuation to the (mixed) volume of some polyhedron in $New(f)$. First let us define the notion of mixed volume:

Definition 7.4. Let P_1, \dots, P_n be bounded polyhedra in \mathbb{R}^n . The Minkowsky sum of P_1, \dots, P_n is

$$P_1 + \dots + P_n = \{v_1 + \dots + v_n \mid v_i \in P_i\}.$$

For $\lambda \in \mathbb{R}_{\geq 0}$, we set $\lambda P_i = \{\lambda v \mid v \in P_i\}$. We define the function

$$\begin{aligned} V_{P_1 \dots P_n} : \mathbb{R}_{\geq 0}^n &\longrightarrow \mathbb{R} \\ (\lambda_1, \dots, \lambda_n) &\longmapsto \text{vol}(\lambda_1 P_1 + \dots + \lambda_n P_n) \end{aligned}$$

where vol is the usual Euclidean volume. The function $V_{P_1 \dots P_n}$ is actually a homogeneous polynomial in $\lambda_1 \dots \lambda_n$ of degree n . The mixed volume $MV(P_1 \dots P_n)$ is defined to be the coefficient of the $\lambda_1 \dots \lambda_n$ -term of $V_{P_1 \dots P_n}$.

Remark. The function MV is monotonic. So, if $P_1, \dots, P_n \subset P$,

$$MV(P_1, \dots, P_n) \leq MV(P, \dots, P) = \text{Vol}(P).$$

Theorem 7.5 (J. Rabinoff [6]). *Let $f_1, \dots, f_n \in \mathbb{Z}_p\langle P \rangle$. Assume that $\bigcap_i V(f_i)$ is finite. Then for all $\nu \in \bigcap_i \text{Trop}(f_i) \cap \mathbb{R}^n$ isolated, let $\check{\gamma}_i = \pi(\text{vert}_\nu(f_i)) \in \text{New}(f_i)$. Then*

$$\left| \bigcap_i V(f_i; \{\nu\}) \right| \leq MV(\check{\gamma}_1, \dots, \check{\gamma}_n).$$

We will now prove that if $f_1, \dots, f_n \in \mathbb{Z}_p\{\overline{X}, \overline{Y}\}$ and their derivatives have an effective Weierstrass bound then uniformly over the parameters \overline{y} , we can compute a bound on the number of isolated points in $\bigcap \text{Trop}(f_i)$ and on the number of zeros in $\bigcap_i V(f_i)$ with tropicalization ν (for a fixed isolated valuation ν in $\bigcap \text{Trop}(f_i) \cap \mathbb{R}^n$).

The key result is that we can compute a set in which lives the support of $\text{New}(f)$:

Lemma 7.6. *Let $f \in \mathbb{Z}_p\{\overline{X}, \overline{Y}\}$ such that f and all its derivatives have an effective Weierstrass bound. Then, we can effectively find an integer $E(f)$ such that for all $\overline{y} \in \mathbb{Z}_p^m$, either $f_{\overline{y}}(\overline{X}) := f(\overline{X}, \overline{y})$ is identically zero or $\text{New}(f_{\overline{y}}) \subseteq B_{\max}(E(f))$.*

In this lemma, $B_{\max}(E)$ denotes the set $\{I \in \mathbb{R}^n \mid \max_k \{i_k\} \leq E\}$. Note also that we have identified $\text{New}(f)$ and its support.

Proof. Let us recall that an element of $\text{New}(f)$ is the projection of a set $\text{vert}_\nu(f)$ (for $\nu \in \mathbb{R}^n$, $\nu = \text{trop}(\overline{x})$ for some $\overline{x} \in (\mathcal{O}_p^*)^n$) i.e. is the set of indexes J such that $v(a_J(\overline{y})) + \langle \nu, J \rangle$ reaches the minimum of the set $\{v(a_I(\overline{y})) + \langle \nu, I \rangle; I \in \mathbb{N}^n\}$ for some $\nu \in [0, \infty)^n$. So, it is sufficient to show that for all $\nu \in [0, \infty)^n$ the projection of the set $\text{vert}_\nu(f)$ is contained in $B_{\max}(E(f))$ for suitable (computable) $E(f)$.

As f has an effective Weierstrass bound, we know that there exists $d(f)$ (computable) such that for all $|I| \geq d(f)$,

$$a_I(\overline{Y}) = \sum_{|J| < d(f)} b_{IJ}(\overline{Y}) a_J(\overline{Y}),$$

where $b_{IJ} \in \mathbb{Z}_p\{\overline{Y}\}$ with $\|b_{IJ}\| < 1$. Fix $\overline{y} \in \mathbb{Z}_p$ and assume $f_{\overline{y}} \neq 0$ i.e. $a_I(\overline{y}) \neq 0$ for some $|I| < d(f)$. First, let us remark that for all I such that $i_1, \dots, i_n \geq d(f)$, for all $\overline{x} \in (\mathcal{O}_p^*)^n$, we can find J with $|J| < d(f)$ such that

$$\begin{aligned} v(a_I(\overline{y})) + \langle I, \text{trop}(\overline{x}) \rangle &\geq \min_{|K| < d(f)} \{v(b_{IK}(\overline{y})) + v(a_K(\overline{y})) + \langle K, \text{trop}(\overline{x}) \rangle\} \\ &> v(a_J(\overline{y})) + \langle J, \text{trop}(\overline{x}) \rangle. \end{aligned}$$

If $n = 1$, take $E(f) = d(f)$ and we are done by the above inequality.

In the general case, we already know by the above inequality that no index I that satisfies $i_1, \dots, i_n \geq d(f)$ can be a point of $\text{vert}_\nu(f)$. It remains to bound indexes in $\text{vert}_\nu(f)$ with at least one coordinate less than $d(f)$.

Fix $1 \leq k \leq n$ and $1 \leq s \leq d(f)$. Fix a coefficient I whose k th coordinate is s . Then, $a_I(\bar{y})\bar{X}^I$ is the $(i_1, \dots, i_{k-1}, s, i_{k+1}, \dots, i_n)$ th coefficient of the function $f_{s,k}(\bar{X}, \bar{y})X_k^s$ where

$$f_{s,k}(\bar{X}, \bar{y}) = (1/s!) \frac{\partial^s f}{\partial x_k^s}(X_1, \dots, X_{k-1}, 0, X_{k+1}, \dots, X_n, \bar{y}).$$

Then, as $f_{s,k}$ has an effective Weierstrass bound, there is $d(f, s, k) := d(f_{s,k})$ such that for all I with $\max_{j \neq k} \{i_j\} \geq d(f, s, k)$,

$$v(a_I(\bar{y})) + \sum_{l \neq k} i_l v(x_l) > \min \{v(a_{(j_1, \dots, j_{k-1}, s, j_{k+1}, \dots, j_n)}(\bar{y})) + \sum_{l \neq k} j_l v(x_l)\}.$$

where the min is taken in $\{J' : |J'| = |(j_1, \dots, j_{k-1}, j_{k+1}, \dots, j_n)| < d(f, s, k)\}$. We set:

$$E'(f) = \max_{k \leq n} \max_{s \leq d(f)} \{d(f, k, s), d(f)\}.$$

If $n = 2$, we can take $E(f) = E'(f)$. Otherwise, we can compute $E(f_{s,k})$ for all $s \leq d(f)$ and $k \leq n$ by induction: we proceed like above with $f = f_{s,k}$. Then, we take $E(f) = \max_{s,k} \{E(f_{s,k}), E'(f)\}$. \square

Remark. Note that in the above lemma, we can make vary the parameter \bar{y} over \mathcal{O}_p^m . Then, it does not change the bound $E(f)$. This is also true for all the below result: the bounds we find also works if the parameters vary over \mathcal{O}_p instead of \mathbb{Z}_p .

We can now bound effectively the number of roots of a system f with isolated tropicalization.

Lemma 7.7. *Let $f = (f_1, \dots, f_n) \in (\mathbb{Z}_p\{\bar{X}, \bar{Y}\})^n$ such that f_i and all its derivatives have an effective Weierstrass bound for all i . Then, one can compute integers D_1 and D_2 (depending only on f) such that for all $\bar{y} \in \mathbb{Z}_p^m$, either $\bigcap V(f_i(\bar{X}, \bar{y}))$ is infinite, or $\bigcap \text{Trop}(f_i(\bar{X}, \bar{y})) \cap \mathbb{R}^n$ has less than D_1 isolated points and for each such a point ν , the cardinality of $\bigcap V(f_i(\bar{X}, \bar{y}), \{\nu\})$ is less than D_2 .*

In particular, under these hypotheses, whenever the system f has finitely may solutions in $(\mathcal{O}_p)^n$, it has at most $D_1 \cdot D_2$ solutions in $(\mathcal{O}_p^*)^n$ with isolated tropicalization.

Proof. Assume that we have chosen \bar{y} such that the number of solutions of the system is nonzero and finite. Then, by lemma 7.6, $\text{New}(f_i, \bar{y})$ is contained in $B_{\max}(E(f_i))$. So, for all i and ν , $\check{\gamma}_\nu(f_i) := \check{\gamma}_\nu(f_i(\bar{X}, \bar{y})) \subset B_{\max}(E(f_i))$. As MV is monotonic,

$$MV(\check{\gamma}_\nu(f_1), \dots, \check{\gamma}_\nu(f_n)) \leq MV(B_{\max}(E(f)), \dots, B_{\max}(E(f))) = E(f)^n,$$

where $E(f) = \max_i E(f_i)$. Take $D_2 = E(f)^n$. By theorem 7.5, D_2 satisfies the conditions of our lemma.

Let us recall that the points of $\bigcap \text{Trop}(f_i(\overline{X}, \overline{y})) \cap \mathbb{R}^n$ are determined by a system of linear equations. Each equation corresponds to an half-hyperplane contained in $\text{Trop}(f_i(\overline{X}, \overline{y})) \cap \mathbb{R}^n$ (determined by some γ_ν). As these half-hyperplanes are in bijection with the faces of $\text{New}(f_i)$ (the $\tilde{\gamma}_\nu$'s, see proposition 7.3), we can bound the number of systems:

Consider the polygon contained in $B_{\max}(E(f_i))$ with the maximal number of faces (say this polygon has d_i faces). Note that d_i is computable. Then, $\text{Trop}(f_i(\overline{X}, \overline{y})) \cap \mathbb{R}^n$ has at most d_i half-hyperplanes. So, the number of isolated points contained in the intersection of all $\text{Trop}(f_j(\overline{X}, \overline{y})) \cap \mathbb{R}^n$ is no more than $\prod_i d_i$. We define D_1 to be the product of all d_i 's. \square

We will now use an other theorem of [6] to bound the number of solutions with tropicalization on a general connected component C of $\bigcap_i \text{Trop}(f_i, P)$. The idea of this theorem is that if we apply a small perturbation to the system then the component C becomes a finite set of points \tilde{C} . For each of these points $\nu \in \tilde{C}$, we can bound the number of solution for the system (after perturbation) with tropicalization ν by theorem 7.5. It turns out that by a result of continuity for the roots, the number of roots with tropicalization in C is bounded by the number of roots with tropicalization in \tilde{C} . Therefore, we will be able to bound the number of roots with tropicalization in C . Let us note that that some points in \tilde{C} may now come from branches of $\text{Trop}(f_i, \tilde{P})$ where \tilde{P} denote a polyhedron containing P in its interior. So we will need to count the number of branches γ_ν of $\text{Trop}(f_i, \tilde{P})$. As for the isolated case, this can be done if we are able to bound the number of solution of f_i in a open ball $B(0, R)$ containing \mathcal{O}_p in its interior. We say that a power series $f(X, \overline{Y})$ has an (effective) $B(0, R)$ -Weierstrass bound if f is convergent on $B(0, R)$ and there is a (computable) uniform bound on the number of solution of $f(X, \overline{y})$ in $B(0, R)$ for all \overline{y} such that $f(X, \overline{y})$ is not identically zero.

Definition 7.8. Let $P = \bigcap_i \{v \in \mathbb{R}^n \mid \langle u_i, v \rangle \leq a_i\}$ be a polyhedron in \mathbb{R}^n . A ε -thickening of P is a polyhedron of the form

$$P' = \bigcap_i \{v \in N_{\mathbf{R}} \mid \langle u_i, v \rangle \leq a_i + \varepsilon\}.$$

More generally, if Π is a polyhedral complex, a thickening \mathcal{P} of Π is a collection of polyhedra of the form $\mathcal{P} = \{P' \mid P \in \Pi\}$, where P' is a thickening of P . We set

$$|\mathcal{P}| = \bigcup P' \quad \text{and} \quad \text{int}(\mathcal{P}) = \bigcup \text{int}(P'),$$

where $\text{int}(P')$ denotes the interior of P' .

We will now assume that all the power series we consider are in $\mathbb{Z}_p\langle P \rangle$ for some $P = \prod [r_i, \infty)$ and that furthermore there is an open polyhedron $\tilde{P} = \prod (s_i, \infty)$ containing P in its interior and such that f has a $B(\tilde{P})$ -Weierstrass bound where $B(\tilde{P}) := \{\bar{x} \mid \text{trop}(\bar{x}) \in \prod (s_i, \infty]\}$. This bound will be denoted by $D(f)$. In particular, this implies that $\text{Trop}(f, \tilde{P})$ is a finite union of γ_v .

Let C be a connected component of $\text{Trop}(f)$. Then for all polyhedron $P' = \prod [r'_i, \infty)$ between P and \tilde{P} there is a unique connected component C' extending C .

Let $f_1, \dots, f_n \in \mathbb{Z}_p\langle P \rangle$ be a system of functions like above. Let C be a connected component of $\bigcap_i \text{Trop}(f_i, P)$. Then, if we apply a small perturbation to the system, the component C' becomes a finite set of point:

Lemma 7.9. *Let C be a connected component of $\bigcap \text{Trop}(f_i, P)$. Then there is δ , P' a δ -thickening of P contained in \tilde{P} and \mathcal{P} a thickening of C contained in P' such that $|\mathcal{P}| \cap \bigcap_i \text{Trop}(f_i, P') = C'$. There also exist $v_1, \dots, v_n \in \mathbb{N}$ and $\varepsilon \in \mathbb{Q}_{\geq 0}$ such that for all $t \in (0, \varepsilon]$, the intersection*

$$|\mathcal{P}| \cap \bigcap_i \left(\text{Trop}(f_i, P') + tv_i \right)$$

is a finite set of points contained in $\text{int}(\mathcal{P})$. Furthermore, each of these point is determined by the intersection of affine polyhedra γ_v contained in the tropicalizations $\text{Trop}(f_i, P')$.

The first part of the lemma follows immediately from the definitions. The second part follows from lemma 12.13 in [6] Let us remark that in the above lemma if $\bigcap_i V(f_i, \tilde{P})$ is a finite set then we may assume that for all \bar{x} in this set, $\text{trop}(\bar{x}) \in P'$.

We fix $t \in \mathbb{Q}$ and ξ in some algebraic extension K of \mathbb{Q}_p such that $v(\xi) = t$. We denote by \tilde{f} the image of the map:

$$\begin{aligned} K\langle P \rangle &\longrightarrow K\langle tP \rangle \\ f(x_1, \dots, x_n) &\longmapsto f(x_1\xi^{-1}, \dots, x_n\xi^{-1}). \end{aligned}$$

Then, $\text{Trop}(\tilde{f}) = \text{Trop}(f) + t$. Let us remark that $\text{Trop}(\tilde{f})$ and $\text{New}(\tilde{f})$ are independent of the choice of ξ with $v(\xi) = t$ (as these sets are determined uniquely by the valuations of the coefficients of \tilde{f}).

Definition 7.10. *Let $f_1, \dots, f_n \in \mathbb{Z}_p\langle P \rangle$ be nonzero as before and let $\nu \in \bigcap \text{Trop}(f_i)$ an isolated point. The stable tropical intersection multiplicity of $\text{Trop}(f_1), \dots, \text{Trop}(f_n)$ at ν is defined to be*

$$i(\nu, \text{Trop}(f_1) \cdots \text{Trop}(f_n)) = MV(\check{\gamma}_1, \dots, \check{\gamma}_n)$$

where $\check{\gamma}_i = \pi(\text{conv}(\text{vert}_\nu(f_i))) \in \text{New}(f_i)$. Let $C \subset \bigcap \text{Trop}(f_i, P)$ be a connected component. Let $P', \mathcal{P}, v_1, \dots, v_n, \varepsilon$ be like in lemma 7.9. The stable tropical intersection multiplicity of $\text{Trop}(f_1), \dots, \text{Trop}(f_n)$ along C is defined to be

$$i(C, \text{Trop}(f_1) \cdots \text{Trop}(f_n)) = \sum i(\nu, (\text{Trop}(f_1) + \varepsilon v_1) \cdots (\text{Trop}(f_n) + \varepsilon v_n)),$$

where the (finite) sum is taken over all ν in $|\mathcal{P}| \cap \bigcap_i (\text{Trop}(f_i, P') + \varepsilon v_i)$.

It turns out that this number is well-defined and independent of all choice. Furthermore, we can bound it effectively:

Lemma 7.11. *Let $f_1, \dots, f_n \in \mathbb{Z}_p\{\overline{X}, \overline{Y}\}$ such that for all i , f_i and its derivatives have an effective $B(\tilde{P})$ -Weierstrass bound. Then, we can compute T such that for all \overline{y} , for all connected component C in $\bigcap_i \text{Trop}(f_i(\overline{X}, \overline{y}))$,*

$$i(C, \text{Trop}(f_1), \dots, \text{Trop}(f_n)) \leq T.$$

Proof. Like in lemma 7.6, we can compute a box $B_{\max}(E(f_i))$ such that uniformly over the choice of the parameter, $\text{New}(f_i(\overline{X}, \overline{y}), P')$ is contained in $B_{\max}(E(f_i))$. Let us remark that we have to use now $D(f_i)$ instead of the Weierstrass bound. (Note that $D(f_i)$ is bigger than the Weierstrass bound of the function f_i after a change of variable which send P' to $\prod[0, \infty)$.)

So, as in lemma 7.7, we can compute a maximal number T_1 of half-hyperplan (the γ_ν 's) which cover C' and therefore we can bound the cardinality of $|\mathcal{P}| \cap \bigcap_i (\text{Trop}(f_i, P') + \varepsilon v_i)$ i.e. the number of elements $i(\nu, (\text{Trop}(f_1) + \varepsilon v_1) \cdots (\text{Trop}(f_n) + \varepsilon v_n))$ in the sum in $i(C, \text{Trop}(f_1) \cdots \text{Trop}(f_n))$.

On the other hand, let $f = \sum a_I \overline{X}^I \in \mathbb{Z}_p\{\overline{X}\}$ and $\tilde{f}(\overline{X}) = \sum a'_I \overline{X}^I := f(\overline{X}t^{-v_i})$ (so, for t with $v(t) = \varepsilon$, $\text{Trop}(\tilde{f}_i) = \text{Trop}(f_i) + \varepsilon v_i$). Let \overline{x} with valuation in P' and $t \in \mathcal{O}_p$ with valuation ε and $I \in \mathbb{N}^n$ such that

$$v(a_I \overline{x}^I) = \min_J \{v(a_J \overline{x}^J)\}.$$

Then, for $\overline{x}' = \overline{x}t^{v_i}$,

$$v(a'_I \overline{x}') = v(a_I \overline{x}^I t^{-\langle I, \overline{v} \rangle}) = \min_J \{v(a_J \overline{x}^J t^{-\langle J, \overline{v} \rangle})\} = \min_J \{v(a'_J \overline{x}'^J)\}.$$

Therefore, $\text{New}(f)$ and $\text{New}(\tilde{f})$ are both contained in the box given in lemma 7.6. It means that like in lemma 7.7, we can compute a bound T_2 for $i(\nu, (\text{Trop}(f_1) + \varepsilon v_1) \cdots (\text{Trop}(f_n) + \varepsilon v_n))$ (independent on the choice of ν). Take $T = T_1 T_2$ and we are done. \square

Remark. In the above proof, we see that we have actually computed a bound for the number of branches of $\text{Trop}(f_i(\overline{X}, \overline{y}), P')$. Therefore, if T is like above then

$$\sum_C i(C, \text{Trop}(f_1) \cdots \text{Trop}(f_n)) \leq T$$

where the sum is taken over all connected component C of $\bigcap_i \text{Trop}(f_i(\overline{X}, \overline{y}), P)$.

Let $f_1, \dots, f_n \in \mathbb{Z}_p\langle P \rangle$, $f_i = \sum a_I^{(i)} \overline{X}^I$. Let $\Delta(f_i) = \{I \mid a_I^{(i)} \neq 0\}$ and $\Delta(f) = \bigcap_i \Delta(f_i)$. We say that $\Delta(f)$ is pointed if its convex closure has dimension n .

It turns out that if $\Delta(f)$ is pointed, $i(C, \text{Trop}(f_1) \cdots \text{Trop}(f_n))$ gives a bound for the number of solution of the system (f_1, \dots, f_n) with tropicalization in C . It follows from [6] that

Theorem 7.12. *Let $P = \prod [r_i, \infty)$ and $f_1, \dots, f_n \in \mathbb{Z}_p\langle P \rangle$ as before. Assume that $\bigcap_i \Delta(f_i)$ is pointed. Let C be a connected component of $\bigcap_i \text{Trop}(f_i)$. Then,*

$$\left| \bigcap_i V(f_i; C) \right| \leq i(C, \text{Trop}(f_1) \cdots \text{Trop}(f_n))$$

if the left side is finite.

With this theorem, we are now able to prove the main theorem of this section:

Theorem 7.13. *Let $f = (f_1, \dots, f_n) \in \mathbb{Z}_p\{\overline{X}, \overline{Y}\}^n$ convergent on a open ball B containing \mathcal{O}_p^n such that f_i and all its derivatives have an effective B -Weierstrass bound for each i . Then, there exists $S(f)$ computable in terms of the f_i 's such that for all $\overline{y} \in \mathbb{Z}_p^n$, either the system $f_{\overline{y}}$ has infinitely many roots or it has less than $S(f)$ roots in $(\mathcal{O}_p^*)^n$.*

Proof. If $\Delta(f)$ is pointed, we are done by lemma 7.11 and theorem 7.12. Let us remark that in this case, the number $S(f)$ is determined using only the effective B -Weierstrass bound of the f_i 's (and their derivatives). Actually, we just need to compute a box like in lemma 7.6.

In order to guarantee that the above polyhedron is pointed, we apply the following transformations to our system:

- If the variable X_i does not occur in f_j , we set $f'_j := f_j \cdot (1 + p^s X_i)$. We apply this transformation for all i, j when necessary. Then, the number of solutions of the system $f' = (f'_1, \dots, f'_n)$ in B is the same that the number of solutions of the system (f_1, \dots, f_n) . Indeed, the polynomial $(1 + p^s X_i)$ has no root in B for s large enough. Also, f'_j has the same effective B -Weierstrass bound that the B -Weierstrass bound of f_j . Note that the box $B_{\max}(E(f'_i))$ in which lies the Newton complex of f'_i does not depend on the choice of s .
- Let $\tilde{f} = (\tilde{f}_1, \dots, \tilde{f}_n)$ be the system obtained after the change of variables $X_i \mapsto X_i - p^t Z_i$ applied to the system (f'_1, \dots, f'_n) (where \overline{Z} is a new parameter). Then, for t large enough, \tilde{f}_j has the same effective B -Weierstrass bound that f_j and f'_j . Also, for a suitable choice of $\overline{z} \in \mathbb{Z}_p^n$, the number of non-zero solutions of the system $(\tilde{f}_1, \dots, \tilde{f}_n)$ is finite and is an upper bound for the number of non-zero solutions

of the system (f_1, \dots, f_n) . Furthermore, for the same choice of \bar{z} , we have that $\Delta(\tilde{f})$ is pointed.

As, $\Delta(\tilde{f})$ is pointed, we can compute a bound $S(\tilde{f})$ on the number of non-zero solutions of the system $(\tilde{f}_1, \dots, \tilde{f}_n)$. Indeed, this number is determined by the effective B -Weierstrass bound of the \tilde{f}_i 's (which are computable as we have discussed above). Note that $S(\tilde{f})$ does not depend on our choices of s, t . We set $S(f) := S(\tilde{f})$. \square

Remark. Let $f_1, \dots, f_{n+m} \in \mathbb{Z}_p\{X_1, \dots, X_n, \bar{Y}\}[X_{n+1}, \dots, X_{n+m}]$ convergent on $B \times \mathbb{C}_p$ and satisfying the hypotheses of the above theorem. Then we can compute a bound for the number of solutions of the system in $(\mathcal{O}_p^*)^n \times (\mathbb{C}_p^*)^m$. Indeed, in this case, the size of the box computed in lemma 7.6 with respect to the variable X_{n+i} is determined by the degree of f_k as polynomial in X_{n+i} . Therefore, using theorem 7.12, for all r_i , we can compute a bound for the number of solution with tropicalization in $P \times \prod_i [r_i, \infty)$ (proceed like in theorem 7.13). Furthermore, we remark that the bound $S(f)$ obtained in this case is independent on the choice of r_i (as so is the box from lemma 7.6) which means that it is a bound for the number of solutions in $(\mathcal{O}_p^*)^n \times (\mathbb{C}_p^*)^m$.

8 Effective model-completeness

We can now prove the second main theorem:

Theorem 8.1. *Let F be an effective family of restricted analytic functions such that the set of \mathcal{L}_F -terms is closed under derivation. Let \tilde{F} be the extension of F by all decomposition functions of elements in F . Assume that each $\mathcal{L}_{\tilde{F}}$ -term is convergent on a open ball $B(f)$ containing \mathcal{O}_p and has an effective $B(f)$ -Weierstrass bound.*

Then, the theory of $\mathbb{Z}_{p, \tilde{F}}$ is effectively strongly model-complete in the language $\mathcal{L}_{\tilde{F}}$.

Proof. For this, as we have seen, it is actually sufficient to prove that $W_{\tilde{F}}$ is an effective Weierstrass system. Let $f \in W_{\tilde{F}, n}^{(k)}$. We have to show that f has an effective Weierstrass bound. We proceed by induction on k and we show that for any $f \in W_{\tilde{F}, n}^{(k)}$, f and each of its derivatives admit an effective Weierstrass bound. The basic step of the induction is proposition 6.4.

So assume that for all n , for all $k \leq m$ and for all $g \in W_{\tilde{F}, n}^{(k)}$, g and all its derivatives have an effective Weierstrass bound. Let $H \in W_{\tilde{F}, n}^{(m+1)}$. We want to compute $d(H)$ (or more generally, $d(G)$ where G denotes a derivatives of H). By definition of the Weierstrass system generated by the $\mathcal{L}_{\tilde{F}}$ -terms, H is a polynomial combination one of the following possibilities:

- (a) $h \in W_{\tilde{F},n}^{(m)}$. In that case, we can compute $d(h)$ by inductive hypothesis.
- (b) There are $f \in W_{\tilde{F},n}^{(m)}$ and a permutation σ such that $h(\overline{X}) = f(X_{\sigma(1)}, \dots, X_{\sigma(n)})$. In that case, we can compute $d(f)$ by inductive hypothesis and $d(h) = d(f)$. The same holds for any derivative of h .
- (c) There is $f \in W_{\tilde{F},n}^{(m)}$ such that f is invertible in $\mathbb{Z}_p\{\overline{X}\}$ and $h = f^{-1}$. In that case, $d(f) = d(h) = 1$. Also, $d\left(\frac{\partial h}{\partial X_i}\right) = d\left(-\frac{\partial f}{\partial X_i}h^2\right) = d\left(\frac{\partial f}{\partial X_i}\right)$ and similarly for the higher derivatives.
- (d) There are $f \in W_{\tilde{F},n}^{(m)}$ and $k \in \mathbb{Z}$ such that $h = f/k$. In that case, we can compute $d(f)$ by inductive hypothesis and $d(h) = d(f)$. The same holds for any derivative of h .
- (e) There are $f \in W_{\tilde{F},n+1}^{(m)}$ of order d in X_{n+1} and $g \in W_{\tilde{F},n+1}^{(m)}$ such that h is one of the functions $a_0, \dots, a_{d-1} \in \mathbb{Z}_p\{X_1, \dots, X_n\}$ or $Q \in \mathbb{Z}_p\{X_1, \dots, X_{n+1}\}$ given by the Weierstrass division theorem.

In the last case, h (or any of its derivatives) is actually determined by a system of equations (see claims 1 to 3 in proposition 5.1). More generally, let $h(\overline{X}) = P(\overline{X}, a_0(\overline{X}), \dots, a_s(\overline{X}))$ where P is any polynomial with coefficients in \mathbb{Z} . Then,

Claim 4. *h and all its derivatives have an effective Weierstrass bound.*

Proof. Let $d(h)$ be the smallest integer like in lemma 6.1. We want to compute a bound of $d(h)$. For this, it is sufficient to bound $S(h)$, the number of roots in \mathcal{O}_p of $h(Z, \overline{y}) = P(Z, a_0(Z, \overline{y}), \dots, a_s(Z, \overline{y}), \overline{y})$, for any $\overline{y} \subset \mathbb{Z}_p^{n+k-1}$ such that this number is finite (where $Z = X_1$ and \overline{y} denotes now $(x_2, \dots, x_{n-1}, y_1, \dots, y_k)$). Fix \overline{y} such that the number of roots is finite. Let us remark that z is a solution of $h(Z, \overline{y}) = 0$ if $z, t_0, \dots, t_s, a_0, \dots, a_s$ are solutions of the system of equations:

$$\left\{ \begin{array}{l} f(t_0, z, \overline{y}) = 0 \\ \vdots \\ f(t_s, z, \overline{y}) = 0 \\ \begin{pmatrix} 1 & t_0 & \cdots & t_0^s \\ \vdots & \vdots & & \vdots \\ 1 & t_s & \cdots & t_s^s \end{pmatrix} \begin{pmatrix} a_0 \\ \vdots \\ a_s \end{pmatrix} = \begin{pmatrix} g(t_0, z, \overline{y}) \\ \vdots \\ g(t_s, z, \overline{y}) \end{pmatrix} \\ P(z, a_0, \dots, a_s, \overline{y}) = 0 \end{array} \right.$$

if $t_i \neq t_j$ for all $i \neq j$. To make sure that this last condition is satisfied, we introduce the variables t_{ij} $0 \leq i < j \leq s$ and add to the system the equations:

$$t_{ij} \cdot (t_i - t_j) - 1 = 0.$$

First, let us remark that we can assume that the system has no solution with at least one zero coordinate: Indeed, if we introduce a new parameter \bar{u} and proceed to the changement of variable $X \mapsto X - u$ (for $X \in \{z, t_0, \dots, a_0, t_{01}, \dots, t_{s-1,s}\}$), then for a good choice of \bar{u} in \mathcal{O}_p , the new system has no solution with zero coordinate and the number of solutions of the new system is the same that before.

Note that this system has finitely many solutions in $(\mathcal{O}_p)^{2s+3} \times (\mathbb{C}_p)^{(s^2+s)/2}$ if $h(Z, \bar{y})$ has finitely many solutions in \mathcal{O}_p . Conversely, the number of solution of $h(Z, \bar{y})$ is equal to the sum of the number of the solutions of the different systems taking in account all possible multiplicities of the t_i 's.

So, the number of solution of $h(Z, \bar{y})$ in \mathcal{O}_p is determined by the sum of the number of solutions of systems $(f_1^{(i)}, \dots, f_{N_i}^{(i)})$ where $f_j^{(i)} \in W_{\tilde{F}}^{(m)}$. Going down by induction (which increase the number of systems we have to consider), we can actually assume that the functions $f_j^{(i)}$ are in $W_{\tilde{F}}^{(0)}$ (i.e. are $\mathcal{L}_{\tilde{F}}$ -terms). So, by theorem 7.13 and the remark after, one can compute a bound S_i for the number of solutions of the system $(f_1^{(i)}, \dots, f_{N_i}^{(i)})$. Take $S = \sum S_i$. Then S is a bound for $d(h)$.

Let h' be a derivative of h . We can compute $d(h')$ in a similar way using the definitions given in the claims 2 and 3 in proposition 5.1. \square

The cases where h is equal to a function Q like in (e) or one of its derivative is obtained similarly using systems given in proposition 5.1. With the same argument, we can compute $d(H)$ for a general function in $W_{\tilde{F},n}^{(m+1)}$. Indeed, H is just a polynomial combination of functions of type (a)-(e) and so is also determined by a system of equations whose functions (and their derivatives) have an effective Weierstrass bound. \square

9 Application: effective model-completeness of the p -adic exponential ring

Let us recall that the natural exponential function $\exp(x) = \sum x^n/n!$ is convergent iff $v(x) > 1/(p-1)$. Unlike the real field, the p -adic field does not carry a natural structure of exponential field. Yet we can use $\exp(X)$ to define a structure of exponential ring: Let E_p be the map $\mathbb{Z}_p \rightarrow \mathbb{Z}_p : x \mapsto \exp(px)$ (if $p \neq 2$, in the other case, we set $E_2(x) = \exp(4x)$). It induces a structure of exponential ring on \mathbb{Z}_p i.e. $(\mathbb{Z}_p, +, \cdot, 0, 1, E_p)$ is a ring and E_p is a morphism of groups from $(\mathbb{Z}_p, +)$ to $(\mathbb{Z}_p^\times, \cdot)$. This structure is a natural equivalent to the structure $(\mathbb{R}, +, \cdot, 0, 1, <, \exp|_{[-1,1]})$. It is known that the real exponential field is decidable if Schanuel's conjecture is true. We use the results of this paper as a first step to a p -adic equivalent result. In this

section, we apply our results to the set $F = \{E_p\}$. In this case we denote the language \mathcal{L}_F by \mathcal{L}_{exp} .

The model-completeness in this case was first done by A. Macintyre in [4]. A first easy observation is that we don't need to add all decomposition functions. Indeed, let $K = \mathbb{Q}_p(\alpha)$ and $V = \mathbb{Z}_p[\alpha]$. As, $E_p(\sum \alpha^i x_i) = \prod E_p(\alpha^i x_i)$, it is sufficient to add to our language the functions $c_{i,j}$ such that:

$$E(\alpha^i x) = c_{0,i}(x) + \cdots + c_{d-1,i}(x)\alpha^{d-1}.$$

Let \mathcal{L}_{pEC} be the expansion of the language \mathcal{L}_{exp} by the functions like above for all finite algebraic extensions K_n (where $(K_n)_{n \in \mathbb{N}}$ is the tower of extensions defined in section 4). Let \mathbb{Z}_{pEC} be the structure with underlying set \mathbb{Z}_p and natural interpretations for the symbols of \mathcal{L}_{pEC} . Then, by theorem 5.2,

Theorem 9.1 (Macintyre [4]). *$Th(\mathbb{Z}_{pEC})$ is strongly model-complete.*

Using an induction on the complexity of the exponential terms, Macintyre also proves that

Lemma 9.2 (Macintyre [4], see also [5]). *Each \mathcal{L}_{pEC} -term f has an effective $B(f)$ -Weierstrass bound.*

So, by theorem 8.1,

Theorem 9.3. *$Th(\mathbb{Z}_{pEC})$ is effectively strongly model-complete.*

So, the decidability of the full theory of $Th(\mathbb{Z}_{pEC})$ or of the p -adic exponential ring is reduced to the decision problem for \mathcal{L}_{pEC} -existential formula. In a subsequent paper, the author will solve this problem assuming a p -adic version of Schanuel's conjecture.

References

- [1] J. Denef. The rationality of the Poincaré series associated to the p -adic points on a variety. *Inventiones Mathematicae*, Vol. 77, No.1, pages 1–24, 1984.
- [2] J. Denef and L. van den Dries. p -adic and Real Subanalytic Sets. *The Annals of Mathematics, Second Series*, Vol. 128, No.1, pages 79–138, 1988.
- [3] L. Lipshitz. Rigid subanalytic sets. *American Journal of Mathematics*, Vol. 115, No. 1, pages 77–108, 1993.
- [4] A. Macintyre. The elementary theory of p -adic exponentiation. Unpublished notes.

- [5] N. Mariaule. *On the decidability of the p -adic exponential ring*. PhD thesis, University of Manchester, 2013.
- [6] J. Rabinoff. Tropical analytic geometry, Newton polygons, and tropical intersections. *Advances in Mathematics*, Vol. 229, no. 6, pages 3192–3255, 2012.
- [7] L. van den Dries. On the elementary theory of restricted elementary functions. *The Journal of Symbolic Logic*, Vol. 53, no.3, pages 796–808, 1988.

Nathanaël Mariaule

Seconda Università di Napoli, Caserta, Italy

E-mail address: NATHANAELJEAN.MARIAULE@unina2.it